NFS Lab 5: NAT, PAT

I Introduction

This lab session will dive into the configuration of a small network using the Cisco Packet Tracer tool and the setup of NAT translations.

I.1 Prerequisites

For this lab, you must install the following tools:

- Cisco Packet Tracer (available for Windows, Mac, and Ubuntu (before 24.04)).

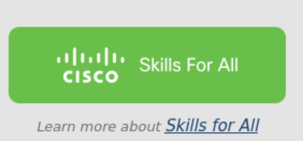
To do so, you can download it from here https://www.netacad.com/courses/getting-started-cisco-packet-tracer.

If you are on linux, you can pull the following self-contained docker image:

```
~$ docker pull farhatizakaria/packettracer  # download the docker image
~$ xhost +local:docker # allow docker to use your linux X server (for GUI display)
~$ docker run -it --name packettracer-container \   # run packet tracer
    -e DISPLAY=$DISPLAY \
    -v /tmp/.X11-unix:/tmp/.X11-unix:rw \
    farhatizakaria/packettracer
~$ docker start packettracer-container && \
  docker exec -it packettracer-container packettracer # alternative command to
start the docker
```

Note: In both cases you will need to register to cisco. You can use a dummy mail address using https://temp-mail.org/en/.

In the docker, you need to connect to your account using the following button for firefox to work correctly in the docker:



II Building the Network

In this part, you will create the network topology and make the basic configuration for the lab.

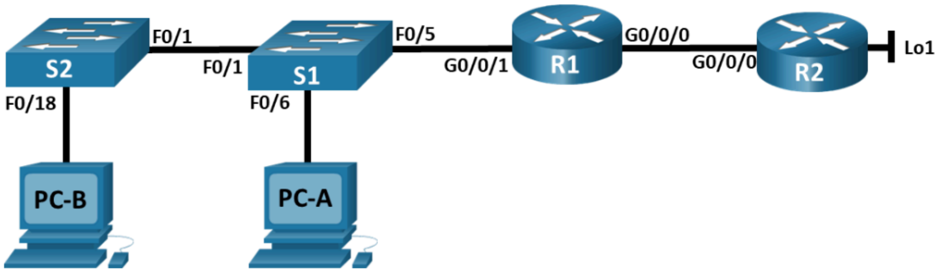
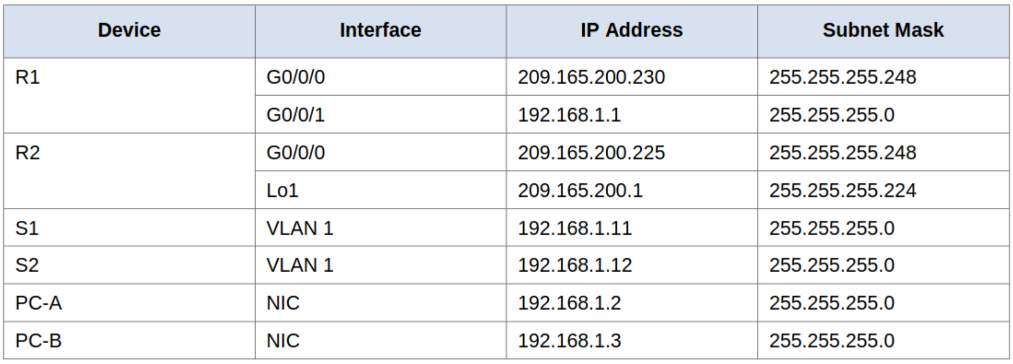


Figure 2: Network Topology.



Device	Interface	IP Address	Subnet Mask
R1	G0/0/0	209.165.200.230	255.255.255.248
	G0/0/1	192.168.1.1	255.255.255.0
R2	G0/0/0	209.165.200.225	255.255.255.248
	Lo1	209.165.200.1	255.255.255.224
S1	VLAN 1	192.168.1.11	255.255.255.0
S2	VLAN 1	192.168.1.12	255.255.255.0
PC-A	NIC	192.168.1.2	255.255.255.0
PC-B	NIC	192.168.1.3	255.255.255.0

Figure 3: Addressing Table.

II.1 Setup

On cisco packet tracer, you need to use the following devices for the lab. Make sure to match the topology above and interfaces from the addressing table.

In the Packet Tracer, you will need to chose between various devices:

For routers and switches:
- 2901 Routers
- 2960 Switches.

For Cables:
- Copper straight through

For Users:
- PC

II.1.1 Setup for Routers

Once your topology and interfaces are linked you can start the configuration of routers by double clicking on them and going to the CLI tab. You will enter the same interface then with minicom in lab 2.

For routers, you will need to do the following:

- Assign the name of the devices.
- Disable the DNS lookup (cf. your cisco cheat sheet from lab 2).
- Configure the IP addresses of the interfaces.
- Define a default route from R1 to R2.

II.1.2 Setup for the Switches

For switches, you will need to do the following:

- Assign the name of the devices.
- Disable the DNS lookup.
- Configure the IP addresses of the interfaces.
- For the remaining interfaces, what good practice should you do?
  - Then do it.

III Configuring NAT for IPv4

In this part, you will configure Network Address Translation (NAT) on router R1. You will use a pool of three public IPv4 addresses and verify the translation process by sending ICMP traffic from multiple LAN devices.

Checkpoint: Call your lab supervisor to show your configuration.

III.1 Setup NAT on R1

III.1.1 Define an access list for inside local addresses

This access list identifies which internal devices are allowed to be translated. In this topology, all hosts on the R1 LAN (192.168.1.0/24) should be eligible.

```
R1(config)# access-list 1 permit 192.168.1.0 0.0.0.255
```

III.1.2 NAT IP pool

For our NAT to work, we need to define a pool of available IP addresses.

- By using the **ip nat** command, create a pool with IPs 209.165.200.226 to 209.165.200.228 with the proper mask.

Like this, the pool cannot be used for NAT, you need to link the inside part of the NAT to your access list 1 to the pool.

- Take a look at the **ip nat inside** command.

III.1.3 NAT Interfaces

Finally, you need to associate each interface of R1 with the inside and the ouside of the nat based the network faced.

- the inside part for the interface facing the LAN.
- outside for the one facing the outer network.

III.1.4 Test your NAT

Using the PC-B command line, try to ping R2′s loopback (209.165.200.1).

On R1:

```
R1# show ip nat translations
```

Question 1: What was the inside local address of PC-B translated to?

Question 2: Try to ping the same IP of R2 from different devices. What can you observe?

III.1.5 Clean up

Before the next part, you need to clear the nat setup using the following command:

```
R1# clear ip nat translations *
```

IV Configuring PAT for IPv4

In this part, you will replace the previous NAT configuration with Port Address Translation (PAT). First, you will configure PAT using a pool of addresses, and then you will configure PAT using the router’s interface IP. You will verify each configuration by generating traffic from multiple hosts.

IV.1 Setup on R1

IV.1.1 IP Pool

Another name of PAT, is NAT overload. In order to allow multiple hosts to share the same IP address we need to modify unlink our previous list 1 and pool and relink it with the overload argument.

To unlink the previous configuration:

```
R1(config)# no ip nat inside source list 1 pool PUBLIC_ACCESS
```

For the overload, try to retake a look at the **ip nat inside** command.

IV.1.2 Test your PAT

Using the PC-A command line, try to ping R2′s loopback (209.165.200.1).

Check the nat translation again.

Question 3: What was the inside local address of PC-A translated to?

Question 4: Try to ping the same IP of R2 from different devices. What can you observe in the translation?

Acknowledgements

This work is inspired by Cisco network academy labs.